文章编号:1000-5862(2020)06-0639-05

资源池安全接入管理关键技术研究

杨 波[1],马 勇[2*],马志程[3],邵诗韵[2],杨仕博[3],王明文[2]
(1. 国网甘肃省电力公司信息通信公司,甘肃 兰州 730050;2. 江西师范大学计算机信息工程学院,江西 南昌 330022;
3. 甘肃同兴智能科技发展有限责任公司,甘肃 兰州 7300502)

摘要: 为保证在虚拟机中的桌面或服务器操作系统的安全运行,将安全工作划分为 6 个子任务,提出了以虚拟机管理器工作机制为技术基础、利用代理技术实现主控服务器和宿主服务器之间安全管控与审计,同时提出了虚拟机安全隔离的设计机制,从运行、CPU、内存、存储和网络 5 个方面分析了虚拟机的隔离方式,有效地实现了终端的安全接入管理与隔离运行,为安全审计、抗逃逸攻击等提供了基础安全保障机制.

关键词: 云计算; 服务器虚拟化; 资源池; 代理
中图分类号: TP 319 **文献标志码:** A **DOI:** 10.16357/j.cnki.issn1000-5862.2020.06.16

0 引言

作为云计算应用和运行的重要保障,云安全已经成为云计算领域中被高度关注且亟须克服的技术壁垒. 而由于终端接入是云环境中最主要的攻击来源,以保护并维持数据的机密性、完整性以及可用性为目标,必须设计并建立相对应的安全保护机制以及体系结构[1-2]. 云安全联盟[3]于 2011 年 11 月发布的《云计算服务安全实践手册》全面地总结了在云计算中广泛应用的安全控制模型和技术架构模型. 对控制技术保护相关信息资源的检索和访问是云计算中 IaaS[4]、PaaS[5]和 SaaS[6]的必需手段. 而为了避免侧通道攻击事件的发生,虚拟机之间的通信任务也需要通过访问控制机制实现加强安全保障的目的[7]. 访问控制模型指的是以特定的访问策略为依据对安全系统进行描述并建立安全性的方法. 通过访问控制模型,用户可获取一定程度的云环境资源访问权限,在这些访问控制模型中,用户静态分配权限的占有率较高. R. K. Thomas 等[8]从面向任务的角度出发,提出了一项基于任务的访问控制模型(TBAC),该模型实现了不同工作流或统一工作流的不同访问实例对应采用不同的访问控制策略[9]的工作机制. 文献[10]针对企业级数据仓库的关键问题,基于 DAMT 构建了一种利用所给的关键路径模式,使企业管理决策者能快速掌握信息的工作机制. 文献[11]设计出一种用于分布式计算环境下使用控制的实施方案,但是在授权管理方面较为复杂.

Amazon[12]云平台的数据管理通过 S3 提供可靠网络存储服务. 微软云[13]访问控制管理主要体现共享数据签名和块策略. Google[14]访问控制技术通过向每一位用户提供唯一的用户 ID,用于实现对用户在 Google 云上活动记录的识别任务. 在开源平台中 OpensStack[15]、CloudStack[16]、Eucalyptus[17]等均具有较高的安全性,可以有效区分用户级别和权限,以保证虚拟机严格按照策略进行访问,且 3 者均设置了安全组. 安全组是一个集合,其元素主要包含一些规则,常被管理员或是授权用户进行设置实现对虚拟机访问量的限制.

以上研究较好地解决了基于用户角色的强制访问控制策略的问题,然而基本没有考虑云计算的新特点给传统的访问控制技术带来的挑战,将访问控制服务与 SaaS 相结合较少. 在实际的应用中,IaaS 如果加以隔离机制可以较好地简化企业资源池的访问控制机制,有效加强了设计态和运行态的访问控制.

收稿日期: 2020-05-16
基金项目: 国家自然科学基金(61876074),江西省重点研发计划(20181A50029)和江西省重大科技研发计划(20192AEI91005)资助项目.
通信作者: 马 勇(1977-),男,河南焦作人,教授,博士,主要从事云计算以及人工智能研究. E-mail: mywuda@126.com

1 虚拟化安全接入管理设计

安全虚拟化基础架构平台的核心安全目标是保证在虚拟机中的桌面或服务器操作系统的安全运行和整体安全保密防护,将安全工作划分为 6 个子任务:应用安全、访问安全、数据安全、主机安全、虚拟机安全、物理安全,各任务之间的主要安全支撑关系如图 1 所示.

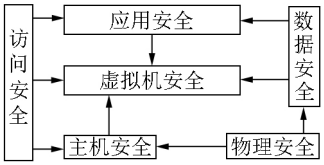

图 1 系统总体安全设计图

应用安全是用户最直接的安全体验,数据安全和访问安全主要通过应用安全体现. 应用安全主要体现通过身份标识和身份认证表明合法用户登录系统,通过授权管理保证用户在完成业务需求的情况下授予最小权限. 访问控制确保合法用户在许可的范围内访问资源和操作业务. 日志审计主要是为了实现详实记录用户的操作目的,方便进行事后审计和即时报警等.

虚拟机安全起到了承上启下的关键作用,构建了应用安全和主机安全的纽带和桥梁. 在裸设备上采用 Linux 或 KVM 虚拟机架构,其主要原理是运用虚拟处理器指令实现对虚拟机之间的隔离性的保障;通过磁盘和网络加密,防止恶意用户攻击.

数据安全确保数据存储安全和访问安全. 存储安全采用云计算资源高度兼容,多个环节采用冗余设计,避免出现单点故障. 客户端通过 SSL 服务访问服务器,以加密的形式传输数据. 在服务器端采用安全数据库和加密等安全机制保证系统数据、虚拟机镜像等数据的机密性、完整性和可用性.

远程管理安全主要分为网络访问安全、API 访问安全和 Web 访问安全. 网络访问安全实现在用户访问云资源时通信信息的安全性和机密性,与应用安全相结合确保合法用户许可操作. Web 安全在网络访问安全基础上防止权限漏洞、会话漏洞、注入漏洞等,提升 Web 代码安全机制能力. API 访问安全与应用安全相结合,支持服务 API 在调用前进行用户或身份验证和权限验证,提升 API 接口安全传输能力等.

主机是云环境下运行的主要单元,也是主机安全的主要载体. 采用强制访问控制机制对系统访问进行权限匹配和虚拟机的强隔离保护,阻止虚拟机逃逸攻击主机和其他虚拟机;通过限制虚拟机直接调用主机计算、网络以及存储资源的技术策略,阻止恶意用户从虚拟机发起 DOS 攻击.

物理安全是其他安全体制的先决条件,主要分为物理设备信息安全和运行安全. 采用磁盘加密、电磁干扰、防电磁信息泄露等技术,防止传输截获等底层安全机制,提升设备信息安全. 以硬件资源统一管理和调度,避免物理设备的单点故障,提升设备的运行安全.

2 虚拟化技术安全设计

2.1 虚拟机管理器安全设计

虚拟机管理器(Hypervisor)是一种提供底层机器虚拟化的软件层. 虚拟化平台系统旨在提供基于 Linux 内核的 KVM 虚拟机服务,属于第 1 类型的虚拟机管理器(Hypervisor). 如图 2 所示,每个宿主服务器需要安装 Agent 程序,Agent 程序定时获取多种监控和审计日志信息发送给主控服务器,主控服务器将数据存储至数据库,形成系统监控和审计日志,通过对比 Hypervisor 的版本和特征值,形成防篡改信息. 监控和审计日志获取方式如下:(i)读取强制访问控制(MAC)的日志文件后抽取 MAC 越权信息;(ii)读取系统用户登录日志文件形成审计日志;(iii)调用 Hypervisor 的接口获取运行监控数据(包括 CPU、内存信息);(iv)调用 Hypervisor 的接口获取其版本和特征值信息,进而形成防篡改审计信息. 具体安全设计内容如下:

1)虚拟机管理器定制. 虚拟化平台系统的虚拟机管理器(Hypervisor)基于 Linux 内核进行定制,去除了与虚拟化不相关的功能模块,并对已知的 Linux 内核安全漏洞进行了修复,提升并保障了虚拟机管理器的安全性能.

2)禁止特权用户登录. 虚拟化平台系统通过安全访问控制策略来限制系统用户的登录行为,系统只允许指定的非特权用户进行登录,所有非授权用户的登录操作(包括本地/远程)都将被系统拒绝.

3)禁止所有远程管理服务. 虚拟化平台系统是基于裸金属架构建立的,在系统定制过程中未携带与远程管理相关的服务软件(如 SSH、TELNET 等). 因此,系统本身不提供任何形式的远程管理功能的

客观因素导致用户无法从远程登录系统进行操作.

4) 宿主服务器用户登录审计. 虚拟化平台系统对宿主服务器中的所有用户登录事件进行审计,当系统检测到有用户登录到宿主服务器时,系统将记录该用户的登录信息并在系统管理界面进行警告.

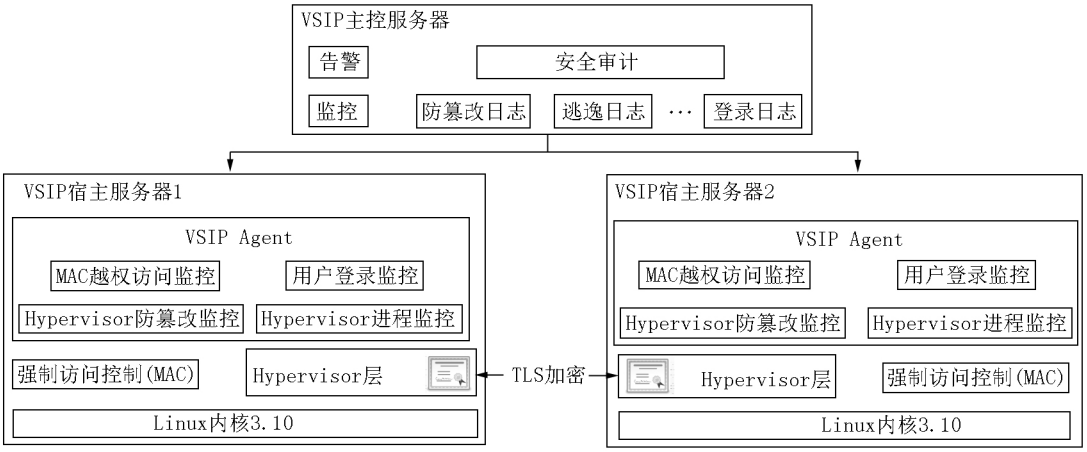

图 2　虚拟机管理器安全管理设计

5) 宿主服务器强制访问控制. 虚拟化平台系统通过利用强制访问控制(MAC)策略实现对宿主服务器资源严密的安全限制. 由于强制访问控制对传统的访问控制列表(ACL)在资源安全保障方面做了提升,即在强制访问控制模式下,系统自动为每一个对象添加一个安全上下文标签. 在此基础之上,还设置了严苛的访问条件,只有具备传统的访问控制列表权限并且获得强制访问控制策略授权的进程才有系统资源的访问权限.

当系统检测到有越权访问时,会将越权日志记录到特定的系统越权日志文件中,系统会定时扫描越权日志文件中的越权信息,并保存到越权审计日志表中.

6) 虚拟机管理器防篡改. 虚拟化平台系统对宿主服务器中虚拟机管理器(Hypervisor)的版本和特征值进行管理与监控,对异常版本或特征值的宿主服务器中的虚拟机管理器进行警告,并生成审计日志,防止虚拟机管理器被非法篡改.

7) 虚拟机管理器通信加密. 虚拟化平台系统对系统中各宿主服务器上的虚拟机管理器(Hypervisor)间的数据通信使用证书进行加密,以防止通信数据被非法篡改.

2.2　虚拟机安全隔离设计

虚拟机安全隔离提供了虚拟机及相关存储、网络的隔离保护功能,包括虚拟机运行隔离、虚拟机 CPU 隔离、虚拟机内存隔离、虚拟机网络隔离、虚拟机存储隔离等(见图 3).

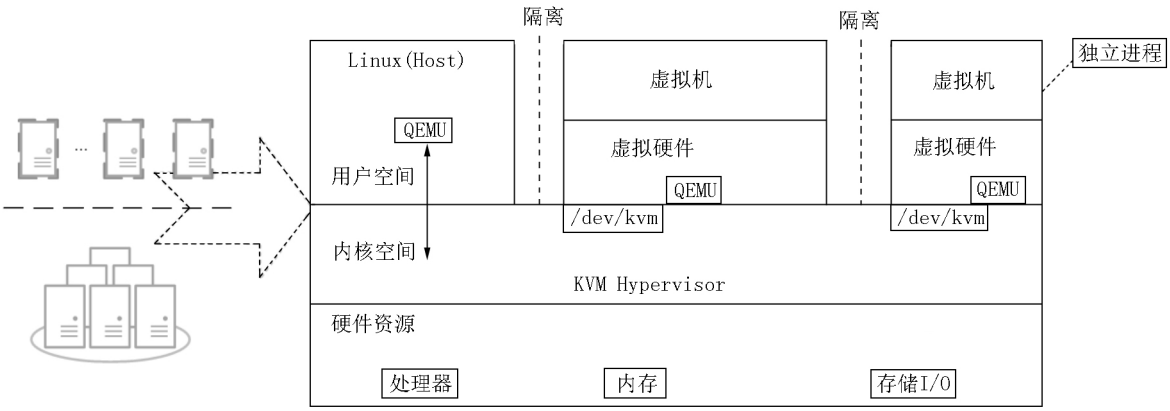

图 3　虚拟机安全隔离逻辑示意图

具体安全隔离设计内容如下:

1) 虚拟机运行隔离. 虚拟化平台系统在同一台物理主机上可以创建并同时运行多台虚拟机,一些相对独立的物理资源都可被每一台虚拟机获取,即若其中某一台虚拟机发生崩溃问题,则虚拟机管理器和其他虚拟机的工作状态不会受到干扰.

2) 虚拟机 CPU 隔离. 为了使得虚拟化指令运行更高效且安全,x86 架构为 CPU 提供了 4 种特权级

别指令,按照优先级降序排列依次为 Ring0(应用于操作系统内核)、Ring1 和 Ring2(应用于操作系统服务)、Ring3(应用于应用程序). 为了防止虚拟机直接执行 CPU 特权指令,并实现在不同虚拟机之间的虚拟处理器(vCPU)指令和处理性能的有效隔离,虚拟机操作系统在虚拟化平台系统的控制下运行在 Ring1 上,其虚拟处理器(vCPU)指令的执行和上下文切换由虚拟化平台进行统一调度.

3) 虚拟机内存隔离. 虚拟化平台系统只允许使用内存独占模式,保证不同虚拟机之间的内存隔离以及独立性,系统保证当物理主机的内存空间都被分配完后,不能够再新建虚拟机.

4) 虚拟机网络隔离. 在虚拟化平台系统中,同一物理主机上不同虚拟机之间的网络隔离可以得到保证,目的地址不是自己的并且非广播报文是无法被虚拟机收到的,其中包括基于 ICMP、TCP、UDP 等协议的非广播报文. 在设置端口组网络策略时,关闭混杂模式(见图 4).

5) 虚拟机存储隔离. 虚拟化平台系统保证虚拟机只有访问分配给该虚拟机的存储空间的权限,一个虚拟磁盘在某一时刻只能被一个虚拟机挂载.

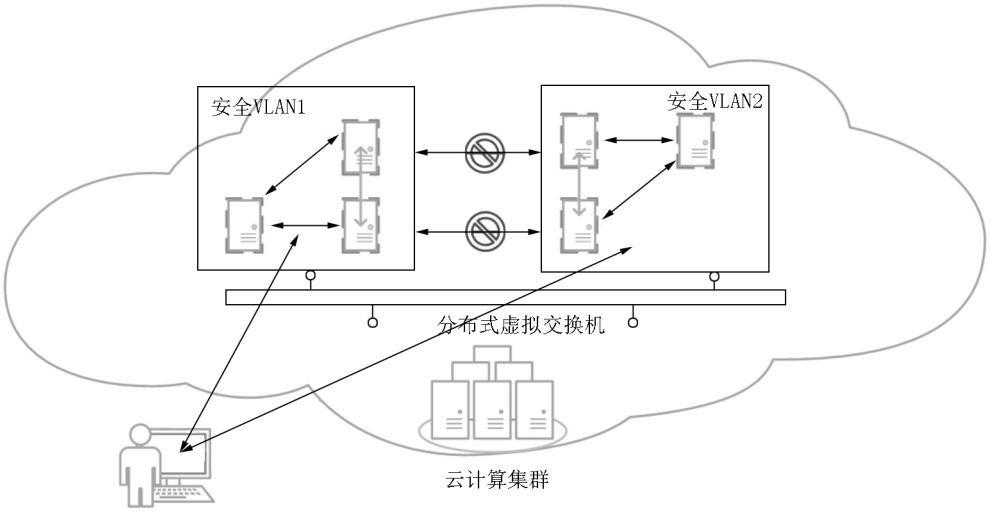

图 4 虚拟机网络隔离示意图

3 结束语

资源池技术在企业的数据管理方面获得的应用越来越广泛,尤其是大型企业的数据中心采用服务器虚拟化的方式构建新型的数据中心基础设施,统一对外提供计算服务. 安全问题成为影响资源池深化应用的主要因素. 本文将安全架构划分为 6 个子任务,设计出了一套面向虚拟机管理器工作机制以及虚拟机安全隔离的解决方案,有效构建了资源池设计和运行环节的精简安全工作机制和模式. 为安全审计、抗逃逸攻击等提供了基础安全保障机制. 下一步工作将主要集中探讨抗虚拟机逃逸攻击和拒绝服务攻击等安全防御的关键技术研究和架构设计.

4 参考文献

[1] Curry S, Darbyshire J, Fisher D W, et al. Infrastructure security: getting to the bottom of compliance in the cloud [J]. RSA Security Brief, 2010, 45(3): 196-204.

[2] Kaur P J, Kaushal S. Security concerns in cloud computing [M]. Berlin: Heidelberg, 2011: 103-112.

[3] Feng Dengguo, Zhang Min, Zhang Yan, et al. Study on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83.

[4] Bhardwaj S, Jain L, Jain S. Cloud computing: a study of infrastructure as a service (IAAS) [J]. International Journal of Engineering and Information Technology, 2010, 2(1): 60-63.

[5] Mell P, Grance T. The NIST definition of cloud computing [EB/OL]. [2019-10-17]. https://www.researchgate.net/profile/Ghulam_Muhammad2/publication/272375651_Automatic_speech_recognition_using_interlaced_derivative_pattern_for_cloud_based_healthcare_system/links/569d2eb308ae950bd7a66995.pdf.

[6] Armbrust M, Fox A, Griffith R, et al. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50-58.

[7] Wang Yuding, Yang Jiahai, Xu Cong, et al. Survey on access control technologies for cloud computing [J]. Journal

of Software,2015,26(5):1129-1150.

[8] Thomas R K,Sandhu R S. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management [M]. Boston: Springer,1998:166-181.

[9] Deng Jibo,Fan Hong. Task-based access control model [J]. Journal of Software,2003,14(1):76-82.

[10] 赵宏斌,白开峰,崔丙锋,等. 基于 DAMT 的企业级数据仓库建设关键路径研究 [J]. 江西师范大学学报: 自然科学版,2018,42(6):88-92.

[11] Wang Xiaowei,Zhao Yiming. A task-role-based access control model for cloud computing [J]. Computer Engineering,2012,38(24):9-13.

[12] Amazon. Using bucket policies and user policies [EB/OL]. [2019-10-11]. http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingIAMPolicies.html

[13] Baike. Windows azure [EB/OL]. [2019-10-11]. http://baike.baidu.com/view/1997158.htm.

[14] Google. Security whitepaper: google apps messaging and collaboration [EB/OL]. [2019-10-11]. https://www.tradepub.com/free/w_aaaa2180/.

[15] NASA,Rackspace. OpenStack [EB/OL]. [2019-10-11]. http://www.openstack.org/.

[16] Apache. CloudStack [EB/OL]. [2019-10-11]. http://cloudstack.apache.org/.

[17] Eucalyptus Systems Inc. Eucalyptus [EB/OL]. [2019-10-11]. https://www.eucalyptus.com/.

The Study on Key Technology of Secure Access to the Resource Pool Management

YANG Bo[1],MA Yong[2*],MA Zhicheng[3],SHAO Shiyun[2],YANG Shibo[3],WANG Mingwen[2]

(1. State Grid Gansu Information and Telecommunication Company,Lanzhou Gansu 730050,China;
2. College of Computer and Information Engineering,Jiangxi Normal University,Nanchang Jiangxi 330022,China;
3. Gansu Shining Science and Technology Company Limitied,Lanzhou Gansu 730050,China)

Abstract: In order to ensure the safe operation of the desktop or operating system in the virtual machine,the security work is divided into six parts. The working mechanism of virtual machine manager is put forward,and the security control and audit between host server and hosting server are realized by proxy technology. The design mechanism of virtual machine security isolation is proposed,and the isolation mode of virtual machine is analyzed in five aspects of operation,CPU,memory,storage and network. The safe access management and isolation operation of the terminal are implemented effectively,providing basic security mechanism for security audit and anti-escape attack.

Key words: cloud computing; server virtualization; resource pooling; agent

(责任编辑: 冉小晓)